# Cyber roadblocks – 5 common misconceptions

## What's cyber liability and privacy protection, and who should buy it?

Cyber liability and privacy protection insurance is designed to address the exposures insureds face when using the internet, email, websites, computer programs and, in particular, from storing private information about their clients.

We often hear that clients don't buy a cyber liability and privacy protection policy because they don't think they have an exposure or because they believe it won't happen to them. To combat these common misconceptions, we've put together some talking points.

# 1. I don't hold valuable data

Valuable data isn't limited to intellectual property. It can be as simple as your employees, suppliers, and even your own personal details, such as your full name, date of birth, driver's licence number, tax file numbers and bank account details.

Most businesses will hold this information about their employees or suppliers as a minimum, meaning they're at a higher risk of being targeted for a cyberattack.

If a cyberattack were to occur and this valuable data is stolen, an attacker may use it to commit identity fraud (such as taking out a loan in someone else's name) or as the basis for a social engineering or phishing attack. When this happens, an insured may have to notify the privacy commissioner, as well as the individuals affected by the attack, that this information has been stolen. There are new criminal offences in this space that carry a maximum fine of $10,000. This includes offences for businesses that fail to notify a privacy breach appropriately and destroy personal information that has been requested.

# 2. I don't transact online

An insured's business may not have a website however most businesses use a computer, a local network, or a server to hold electronic files and records or even hold hard copies of personal and sensitive information on site that may be accessed.

A business may do its banking online, or manage its invoicing, both of which may include sending and receiving personal or sensitive information. An insured may also receive supplier invoices via email, which can be easily accessed in the case of a system breach or cyberattack.

Human error is another reason a data breach can happen. For example, an employee may unknowingly forward an email containing malicious software. They may also accidentally send valuable and sensitive data to an unintended recipient or even leave a hard copy of a sensitive document in a public place.

Data breaches are malicious (criminal) via phishing, hacking, or deliberate malware attacks that only require an internet connection for a hacker to access an inadequately protected system.

# 3. Our data is safe in the cloud

Did you know that an insured is legally responsible for the information stored in their cloud, even if a hacker accesses the cloud via a third party?

A common example is an insured's outsourced information technology (IT) provider. As a result of this, an insured may incur notification costs (to both the privacy commissioner and the affected individuals), remediation costs and legal costs.

Data stored in the cloud can be accessed, copied, stolen or altered just as easily as data stored on a computer or server. Once a breach occurs, the information in the cloud is still classified as 'breached' even though there may be multiple soft copy backups that mirror the data stored in the cloud. Even though the sensitive information hasn't been lost, it has been accessed by an unauthorised party and is still subject to the relevant privacy legislation.

Depending on where a cloud provider is located, varying laws from different jurisdictions around the world may apply to the information held. In this instance, lawyers need to identify which countries' laws apply to which breaches, and what violations of that law have occurred. It doesn't take many competing jurisdictions for this to add up to a very expensive exercise. Depending on the law that applies to the potential breach, there may also be significant fines and penalties against the insured as a result.

# 4. Our IT employee/consultant will take care of it

Does your IT employee or consultant work 24/7? A cyber liability and privacy protection policy offers 24/7 emergency incident response services.

Do theyhave the necessary IT forensic skills and qualifications to investigate this type of incident? A cyber incident response team is made up of individuals who have the experience and global expertise in these fields to help mitigate further loss, mediate complicated situations, and provide the best advice on what action to take next.

# 5. Our IT system can't be breached

## No system is 100% safe.

The world's biggest companies have been breached, including the FBI, Facebook and Sony. If these companies, with massive budgets for high-tech cyber security professionals and products, can be hacked, then it's likely a hacker will be able to gain access to an SME with a relatively small budgets for cyber and data security.

Hackers see SMEs as quick and easy money, because of the low security measures they're able to put in place.

Given the need for security, software developers are constantly issuing 'patches' to help reduce the number of hacks. However, these may not necessarily help in all cases.

Breaches can result from human error, including instances where mobile phones, tablets or laptops are misplaced or lost in public places. If these devices aren't encrypted, they can be easily hacked.

If this happens, an insured may be required to notify the Office of the Australian Information Commissioner (OAIC). Notifying the OAIC of any data breach or cyber security breach involves significant legal costs. SMEs don't usually budget for this due to the belief they're adequately protected against cyber and privacy breaches.

We hope the above information assists in considering these common misconceptions in the market.

# Our WebRater cyber product

## You can now quote and bind in minutes on the WebRater.

Our cyber liability and privacy protection insurance has been designed to address the exposures insureds face from relying on the internet, email, websites, computer programs, data, and from storing private information about their clients. Our WebRater provides instant cyber quotes. If a risk doesn't meet our WebRater underwriting criteria, our financial lines underwriters are ready to help with more complex scenarios.

## Questions?

For further details on our cyber protection, please contact your local DUAL underwriter.

## Helping you do more

New Zealand | +64 9 973 0190

**dualinsurance.com**